代数幾何学シンポジウム記録
1995年度 pp.20-31

COMPLETE INTERSECTION PROPERTY OF HECKE ALGEBRAS

KAZUHIRO FUJIWARA

Nagoya University
Department of Mathematics

§0. Introduction

In [TW], the complete intersection property of minimal Hecke rings is shown. In this paper we present a review of [TW] with technical improvements. A generalization to the totally real case is in preparation. In [TW] a multiplicity one theorem based on q-expansion principle in [W , §2] was needed implicitly. Our analysis will make the role of q-expansion principle much clearer. Moreover our check will show that minimal Hecke rings have the same properties as in the weight 2 case in the non-ordinary higher weight case.

The author thanks Y.Taguchi for some useful information on this subject.

§1. Commutative Algebra

Here we present an abstract formulation of some argument of [TW]. Our method here is influenced by an argument of Faltings on their work.

Let p be a prime, $\mathcal{O}$ the ring of integers of some p-adic field K, and λ the maximal ideal.

Definition.

Let $\mathcal{Q}$ be a set of finite sets of primes. A Taylor-Wiles system $\{T,\ \mathcal{Q},\ \{T_Q\}_{Q\in\mathcal{Q}}\}$ consists of :

TW1) For $q \in Q$, $q \equiv 1 \bmod p$ holds. We put $\Delta_q =$ the p-sylow subgroup of $(\mathbf{Z}/q)^{\times}$ with a generator δ_q, $\Delta_Q = \prod_{q\in Q}\Delta_q$. Then T_Q is a finite local $\mathcal{O}[\Delta_Q]$-algebra.

TW2) T is a finite $\mathcal{O}$-algebra, and $T \simeq T_Q/(\delta_q - 1;\ q \in Q)$ holds as $\mathcal{O}$-algebras for any $Q \in \mathcal{Q}$.

TW3) There is an $\mathcal{O}$-flat T_Q-module M_Q for each $Q \in \mathcal{Q}$ such that M_Q is free of rank α as an $\mathcal{O}[\Delta_Q]$-module for fixed $\alpha \geq 1$.

In [TW], in addition to TW3, the condition that M_Q is a free T_Q-module is required. We just need the weaker assumption here.

Unlike Kolyvagin's Euler systems, we do not impose functoriality in general when the index set grows.

Theorem (Complete intersection theorem).

Assume that a Taylor-Wiles system $\{T, \mathcal{Q}, \{T_Q\}_{Q\in\mathcal{Q}}\}$ *with* $\mathcal{Q} = \{Q_m, m \in \mathrm{N}\}$ *is given.*

a) (growth control) $q \in Q_m \Rightarrow q \equiv 1 \bmod p^m$.

b) (relation control) $r = \mathrm{Card}\, Q_m$ *is independent of* m.

c) (generator control) T_{Q_m} *is generated by at most* r*-elements as an* $\mathcal{O}$*-algebra.*

Under a), b), and c), T *is a complete intersection, and* $\mathcal{O}$*-flat.*

We put $I_n = (p^n, \delta_q^{p^n} - 1;\ q \in Q) \subset \mathcal{O}[\Delta_{Q_m}]$ for $m \geq n$.

$$\mathcal{O}[\Delta_{Q_m}]/I_n \xrightarrow{\sim} \mathcal{O}[S_1, .., S_r]/(p^n, (1+S_1)^{p^n} - 1, .., (1+S_r)^{p^n} - 1)$$

holds by condition a), sending δ_i to $1 + S_i$. By TW3, $M_{Q_m}/I_n M_{Q_m}$ is free of rank α. $A_{n,m}$ = the image of $T_{Q_m}/I_n T_{Q_m}$ in $\mathrm{End}_{\mathcal{O}[\Delta_{Q_m}]/I_n}(M_{Q_m}/I_n M_{Q_m}) \simeq (\mathcal{O}[\Delta_{Q_m}]/I_n)^{\alpha^2}$. The map $\mathcal{O}[\Delta_{Q_m}]/I_n \to A_{n,m}$ is injective since any element in the kernel must annihilate free $\mathcal{O}[\Delta_{Q_m}]/I_n$-module $M_{Q_m}/I_n M_{Q_m}$.

Now we use an idea of Taylor -Wiles constructing a projective system which approximates a power series ring. Consider the following triplet:

1) A finite ring $A_{n,m}$ with embeddings

$$\mathcal{O}[S_1, .., S_r]/(p^n, (1+S_1)^{p^n} - 1, .., (1+S_r)^{p^n} - 1) \overset{\iota_1}{\hookrightarrow} A_{n,m}$$

$$\overset{\iota_2}{\hookrightarrow} (\mathcal{O}[S_1, .., S_r]/(p^n, (1+S_1)^{p^n} - 1, .., (1+S_r)^{p^n} - 1))^{(\alpha \dim_K T\otimes_{\mathcal{O}} K)^2}$$

2) r-generators $f_1, .., f_r$ of $A_{n,m}$ in the maximal ideal as an $\mathcal{O}$-algebra.

3) A quotient ring $B_{n,m} = A_{n,m}/(\delta_q - 1;\ q \in Q_{m(n)})$ with T-algebra structure.

Since the order of $A_{n,m}$ is bounded as m varies, isomorphism classes of triplets $((A_{n,m}, \iota_1, \iota_2), B_{n,m}, \{f_1, .., f_r\})$ are finite, and hence for any infinite set Y there is an infinite set $X_n(Y) \subset Y \cap \{m \in \mathrm{N}; m \geq n\}$ such that $((A_{n,m}, \iota_1, \iota_2), B_{n,m}, \{f_1, .., f_r\})$, $m \in X_n(Y)$, are isomorphic. For $n \geq 1$ we put

$$X(n) = X_n(\cdot\cdot X_2(X_1(\mathrm{N}))\cdot\cdot),\ m(n) = \inf_{m\in X(n)} m.$$

For the increasing sequence $\{m(n)\}_{n\in\mathrm{N}}$ thus obtained $((A_{n,m(n)}, \iota_1, \iota_2), B_{n,m(n)}, \{f_1, .., f_r\})_{n\in\mathrm{N}}$ form a projective system. We put $J_n = \mathrm{Ker}(T_{Q_{m(n)}} \to A_{n,m(n)})$. By taking the projective limit we define

$$P = \varprojlim A_{n,m(n)} = \varprojlim_{n\in\mathrm{N}} T_{Q_{m(n)}}/J_n.$$

By condition 2), there is a surjection $\mathcal{O}[[T_1, .., T_r]] \twoheadrightarrow P$. By 1), P contains $\mathcal{O}[[S_1, .., S_r]] = \varprojlim_n \mathcal{O}[S_1, .., S_r]/(p^n, (1+S_1)^{p^n} - 1, .., (1+S_r)^{p^n} - 1)$ as a sub $\mathcal{O}$-algebra, and $P \subset \mathcal{O}[[S_1, .., S_r]]^{\alpha^2}$ is finite as an $\mathcal{O}[[S_1, .., S_r]]$-module. By the next lemma $P \xleftarrow{\sim} \mathcal{O}[[T_1, .., T_r]]$, and hence P is a power series ring.

Lemma.

For a finite local $\mathcal{O}[[S_1,..,S_r]]$-algebra P of dimension strictly less than $r+1$, $P \supset \mathcal{O}[[S_1,..,S_r]]$ is impossible.

Replacing P by P_{red}, we may assume that P is reduced. Then there is an embedding $P \hookrightarrow \prod_{i\in I} P_i$. Here integral rings P_i define the irreducible components of Spec P. $\dim P_i \leq \dim P$. There is some $i \in I$ such that $\mathcal{O}[[S_1,..,S_r]] \hookrightarrow P_i$ is injective: If not, $I_i = \mathrm{Ker}(\mathcal{O}[[S_1,..,S_r]] \to P_i)$ are non-zero for all $i \in I$. Since $\mathcal{O}[[S_1,..,S_r]]$ is integral $\prod_{i\in I} I_i \subset \cap_{i\in I} I_i$ is not zero, and hence we get a contradiction.

Replacing P by some P_i, we may assume P is integral. By taking the integral closure we may moreover assume that P is integrally closed. Then $\dim P = r+1$ should hold by going up theorem. This is absurd.

From the projective system of exact sequences obtained by 3)

$$(T_{Q_{m(n)}}/J_n)^r \to T_{Q_{m(n)}}/J_n \to T/J_nT \to 0$$

where $(0,..,1,..)$ maps to $\delta_i - 1$, we pass to the limit, and get the exactness of

$$P^r \to P \to T' \to 0.$$

Here $T' = \varprojlim T/J_nT$ is a quotient ring of T. T' is a complete intersection with a presentation as above. Since T' is finitely generated as an $\mathcal{O}$-module, by [Ma] T' is $\mathcal{O}$-flat. We show $T \simeq T'$, thus finishing the proof of the theorem.

Fix $N \geq 1$. Since the transition maps of projective system $\{A_{n,m(n)} = T_{Q_{m(n)}}/J_n\}_{n\in\mathbf{N}}$ are surjective and $T' = \varprojlim T/J_nT$, there is $n \geq 1$ such that

$$A_{n,m(n)}/m^N_{A_{n,m(n)}} \simeq P/m^N_P \simeq \mathcal{O}[[T_1,..,T_r]]/(\lambda, T_1,..,T_r)^N$$

and $T'/m^N_{T'} \simeq (T/J_nT)/m^N_{T/J_nT}$ hold.

The following diagram with exact rows and surjective arrows

$$\begin{tikzcd}
T^r_{Q_{m(n)}} \arrow[r] \arrow[d] & T_{Q_{m(n)}} \arrow[r] \arrow[d] & T \arrow[r] \arrow[d] & 0 \\
(A_{n,m(n)})^r \arrow[r] & A_{n,m(n)} \arrow[r] & T/J_nT \arrow[r] & 0
\end{tikzcd}$$

induces

$$\begin{tikzcd}
(T_{Q_{m(n)}}/m^N_{T_{Q_{m(n)}}})^r \arrow[r] \arrow[d] & T_{Q_{m(n)}}/m^N_{T_{Q_{m(n)}}} \arrow[r] \arrow[d] & T/m^N_T \arrow[r] \arrow[d] & 0 \\
(A_{n,m(n)}/m^N_{A_{n,m(n)}})^r \arrow[r] & A_{n,m(n)}/m^N_{A_{n,m(n)}} \arrow[r] & T'/m^N_{T'} \arrow[r] & 0.
\end{tikzcd}$$

$A_{n,m(n)}/m^N_{A_{n,m(n)}} \simeq \mathcal{O}[[T_1,..,T_r]]/(\lambda, T_1,..,T_r)^N$. On the other hand, $T_{Q_{m(n)}}/m^N_{T_{Q_{m(n)}}}$ is a quotient of $\mathcal{O}[[T_1,..,T_r]]/(\lambda, T_1,..,T_r)^N$ by b). This implies that the left and the middle vertical arrows are isomorphisms. It follows that $T/m^N_T \simeq T'/m^N_{T'}$ for any N, and hence T and T' are isomorphic.

Remark

If $M_Q/(\delta_q - 1;\ q \in Q)M_Q$, $Q \in \mathcal{Q}$, are isomorphic to a unique T-module M, M is a free T-module.

§2. Hecke algebra

First we define the Hecke algebra, which plays the central role in our discussion.

For a subgroup $H \subset (\mathbf{Z}/N\mathbf{Z})^\times$,

$$\Gamma_H(N) = \text{inverse image of } H \text{ under } \Gamma_0(N) \to (\mathbf{Z}/N\mathbf{Z})^\times,$$

$$Y_H(N) = \Gamma_H(N)\backslash\mathcal{H}, \qquad X_H(N) \text{ its compactification}, \qquad J_H(N) := \mathrm{Jac}(X_H(N)).$$

Let $T_H(N)$ be the subring of $\mathrm{End}(\mathrm{Jac}(X_H(N)))$ generated by

$$\begin{cases} T_\ell = T_{\ell *} & \text{for } \ell \nmid N, \\ \langle a \rangle = \langle a \rangle_* & \text{for } (a,N) = 1 \\ U_q = U_{q*} & \text{for } q | N. \end{cases}$$

Let $\pi_i : X_1(N\ell) \to X_1(N)$, $i = 1, 2$, be the map defined by $\pi_1(z) = z$ and $\pi_2(z) = \ell z$ respectively. Then

$$T_{\ell *} = \pi_{2*} \circ \pi_1^* : \ H^1(X_1(N), \mathbf{Z}) \ \to \ H^1(X_1(N), \mathbf{Z}).$$

Also,

$$U_q : \ (E, P) \ \mapsto \ \sum_{C_q \cap \langle P \rangle = \{0\}} (E/C_q, P),$$

where C_q are cyclic subgroups of E of order q.

Let $T_H(N)'$ be the subring of $T_H(N)$ generated by T_ℓ for $\ell \nmid N$ and $\langle a \rangle$ for $(a, N) = 1$ (i.e. omit the U_q's).

Let p be a prime number ≥ 3. For a maximal ideal m of $T_H(N)$ (or $T_H(N)'$) such that $p \in m$, there exists a unique semisimple representation

$$\bar{\rho} : G_\Sigma \ \to \ \mathrm{GL}_2(T_H(N)/m)$$

such that

$$\begin{cases} \operatorname{trace} \bar{\rho}(\mathrm{Fr}_\ell) & = \ T_\ell \\ \det \bar{\rho}(\mathrm{Fr}_\ell) & = \ \ell\langle \ell \rangle \quad \text{for each } \ell \nmid Np. \end{cases}$$

A representation thus obtained is called *modular*.

In this case one finds an $\mathcal{O}$-valued weight 2 modular eigenform $f : T_H(N) \to \mathcal{O}$ with its associated λ-adic representation $\rho_{f,\lambda}$ such that $\bar{\rho}$ is obtained as the reduction modulo λ by extending $\mathcal{O}$ and k. The introduction of H is necessary to put a restriction on the nebentypes of such modular liftings.

In this paper we only consider an absolutely irreducible modular representation $\bar{\rho}$ satisfying local conditions at primes where $\bar{\rho}$ ramifies.

At prime p we impose one of the following:

(Ordinary case) $$\bar{\rho}|_{D_p} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix},$$

where χ_1 and χ_2 are distinct, and χ_2 is unramified. Note that we allow here that $\bar{\rho}|_{I_p}$ is semi-simple.

(flat case) $\bar{\rho}$ comes from a finite flat group scheme over $\mathbf{Z}_p$.

In [W], ordinary case and flat case do not overlap, but here we make one exception. If $\bar{\rho}|_{I_p}$ is ordinary, it comes from a finite flat group scheme if and only if it is semi-simple and $\det\bar{\rho}|_{I_p} = \omega$ (ω is the Teichmüler character), or 1, and we accept it as a flat case in the former case.

If $q \neq p$ then we impose one of the following conditions as in [W]:

(A)
$$\bar{\rho}|_{D_q} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix},$$

where $\chi_1\chi_2^{-1} = \omega$, χ_1 and χ_2 are unramified, and $*|_{I_q} \neq 0$, i.e., the I_q-fixed space is of dimension 1.

(B)
$$\bar{\rho}|_{I_q} \sim \begin{pmatrix} \chi_q & 0 \\ 0 & 1 \end{pmatrix}, \quad \chi_q \neq 1.$$

In the case of elliptic curves, (A) holds if the curve is semi-stable at q and the residual representation is non-trivial. In [W], one more case is considered, but we omit it here for simplicity.

Let $\bar{\rho} : G_\Sigma \to \mathrm{GL}_2(k)$ be an irreducible modular representation, and $M = N(\bar{\rho})$ be the (prime-to p) conductor of $\bar{\rho}$. Then one can find $\bar{\rho}$ as the residual representation of a modular representation $\rho_{f,\lambda} \bmod \lambda$ of level M or Mp (Serre's ϵ-conjecture).

The level is M if $\bar{\rho}$ is flat and $\det\bar{\rho}|_{I_p} = \omega$, and Mp otherwise. We say such a modular representation *minimal*. In the minimal case we take the p-Sylow subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ as H, and put

$$T = (T_H(N) \otimes_{\mathbf{Z}} \mathcal{O})_m,$$

$$T' = (T'_H(N) \otimes_{\mathbf{Z}} \mathcal{O})_m.$$

T, T' are finite flat local $\mathcal{O}$-algebras.

For the later purpose we introduce some notations. For N and q, $(N,q) = 1$, $H \subset (\mathbf{Z}/N\mathbf{Z})^\times$ one puts

$$\Gamma_H(N,q) = \Gamma_{H\times(\mathbf{Z}/q\mathbf{Z})^\times}(Nq) = \Gamma_H(N) \cap \Gamma_0(q)$$

$$Y_H(N,q) = Y_{H\times(\mathbf{Z}/q\mathbf{Z})^\times}(Nq), \ X_H(N,q) = X_{H\times(\mathbf{Z}/q\mathbf{Z})^\times}(Nq).$$

§3. Construction of modular deformations

By Eichler-Shimura, or by Deligne, the existence of λ-adic representation $G_\Sigma \to \mathrm{GL}_2(T' \otimes_{\mathcal{O}} K)$ is known, where T' is a certain Hecke ring. From this, we have a representation with values in $\mathrm{GL}(\Lambda)$, where Λ is a certain T'-lattice. It is quite important to know the existence of Galois representation into $\mathrm{GL}_2(T')$, which can be seen as a deformation of $\bar{\rho}$. By a method of Wiles (method of pseudo-representation) one shows that such a deformation exists provided that the residual representation is irreducible.

Deformations: If we are given $\bar{\rho}$ satisfying the local conditions in §2, we deform it under the following local restrictions.

At p, we assume that the deformation ρ over an artinian local ring is Selmer or flat according to $\bar{\rho}$ is ordinary or flat. By our convention flat $\bar{\rho}$ can be considered ordinary in the exceptional case. Note that any flat deformation in such a case is in fact a Selmer deformation.

At $q \neq p$ where $\bar{\rho}$ ramifies, we put

$$\text{(A)} \qquad \rho|_{D_q} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \quad \psi_i : \text{unramified}, \quad \psi_1\psi_2^{-1} = \epsilon,$$

$$\text{(B)} \qquad \rho|_{I_q} \sim \begin{pmatrix} \chi_q & 0 \\ 0 & 1 \end{pmatrix} \quad \text{with the same } \chi_q \text{ as in §2,}$$

according to $\bar{\rho}$ is type (A) or (B) at q. Let Σ be a finite set of primes including p and all ramifying primes. By $R_{\mathcal{D}}$ we denote the universal deformation ring of $\bar{\rho}$ with deformation data $\mathcal{D} = \{\ \cdot,\ \Sigma,\ \mathcal{O},\ \mathcal{M}\}$, and $\rho^{univ} : G_\Sigma \to \mathrm{GL}_2(R_{\mathcal{D}})$ the universal representation.

Let T' be the Hecke ring with $\{U_q,\ q|N\}$ omitted. $T' \otimes_{\mathcal{O}} K$ is a product of p-adic fields, so we have a representation $\rho_K^{mod} : G_\Sigma \to \mathrm{GL}_2(T' \otimes_{\mathcal{O}} K)$. By Eichler-Shimura, there exists

$$\rho_K^{mod} : G_\Sigma \to \mathrm{GL}_2(T' \otimes_{\mathcal{O}} K)$$

such that

$$\begin{cases} \operatorname{trace} \rho_K^{mod}\,(\mathrm{Fr}_\ell) &= T_\ell \\ \det \rho_K^{mod}\,(\mathrm{Fr}_\ell) &= \ell\langle \ell \rangle \quad \text{for each } \ell \nmid Np. \end{cases}$$

Theorem (Wiles).

Assume that the residual representation of $\rho_K^{mod} : G_\Sigma \to \mathrm{GL}_2(T' \otimes_{\mathcal{O}} K)$ is irreducible. Then there exists

$$\rho^{mod} : G_\Sigma \to \mathrm{GL}_2(T')$$

having the same trace and determinant as ρ_K^{mod}.

Take a basis of $(T' \otimes_{\mathcal{O}} K)^2$ such that

$$\rho_K^{mod}\,(\mathrm{Fr}_\infty) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Here Fr_∞ is the complex conjugation. Then the entries of

$$\rho_K^{mod}(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

have the property that $b(\sigma) \cdot c(\sigma)$ is contained in T' and independent of a choice of basis. Using the irreducibility of $\bar{\rho}$, there exists some τ such that $b(\tau)c(\tau)$ is a unit. Change the basis again so that $b(\tau) = 1$. Then ρ_K^{mod} is defined over T' using this basis.

Proposition.
$T' = T$ holds.

First note that $T' \otimes_{\mathcal{O}} K = T \otimes_{\mathcal{O}} K$, which is proved in [W], chapter 2 §3. (Though $T' \otimes_{\mathcal{O}} K$ is semi-simple, $T \otimes_{\mathcal{O}} K$ can have nilpotent elements so the statement is non-trivial.) The point is that we can recover missing Hecke operators $\{U_q,\ q|N\}$ from the representation ρ^{mod}. It suffices to check that the elements obtained in T' coincide with Hecke operators in $T \otimes_{\mathcal{O}} K = T' \otimes_{\mathcal{O}} K$, which is a product of p-adic fields and hence in case of λ-adic representations.

Proposition.
Assume that $\bar{\rho}$ is a modular representation of type $\mathcal{D}$. Then the representation ρ^{mod} obtained in the theorem is a type $\mathcal{D}$ deformation of $\bar{\rho}$.

Basic idea is that local properties of ρ^{mod} over K are well-understood since it is compatible with local Langlands correspondence [Car].

§4. Construction of a Taylor-Wiles system

By N we mean the level of the Hecke algebra. $\Sigma = \{q;\ q|N\} \cup \{p\}$.

Theorem (Taylor-Wiles).
Assume $\bar{\rho}$ is flat or ordinary at p, and is of type (A), (B) at every $q \neq p$, $q|N$. Then one has a Taylor-Wiles system $\{T, \{T_Q\}_{Q\in\mathcal{Q}_{\Sigma,\bar{\rho}}}\}$ for T with $\mathcal{Q}_{\Sigma,\bar{\rho}} = \{q; q \not| N, q \equiv 1 \bmod p, \bar{\rho}(\mathrm{Fr}_q)$ has distinct eigenvalues $\}$

For $Q \in \mathcal{Q}$ we construct T_Q and M_Q, and verify the conditions of Taylor-Wiles system. Set

$$H' := H \times \text{maximal prime to } p\text{-subgroup of } (\mathbf{Z}/q\mathbf{Z})^\times,$$

$$T_Q := (T_{H'}(Nq_1 \cdots q_r) \otimes_{\mathbf{Z}} \mathcal{O})_{m_Q},$$

where m_Q is the ideal generated by m and $U_{q_i} - \alpha_{q_i}$'s,

$$T_{Q-} := (T_H(N, q_1 \cdots q_r) \otimes_{\mathbf{Z}} \mathcal{O})_{m_Q}.$$

Then we have

$$T_{Q-} \simeq T = (T_H(N) \otimes_{\mathbf{Z}} \mathcal{O})_m.$$

Note that for $q \in Q$, $Q \in \mathcal{Q}_{\Sigma,\bar{\rho}}$, the representation does not occur in the space of forms on $\Gamma_H(N, q)$ which is new at q. If not, $\bar{\rho}(\mathrm{Fr}_q)$ looks like $\begin{pmatrix} \alpha_q & 0 \\ 0 & \beta_q \end{pmatrix}$ with

$\alpha_q/\beta_q = q$, $\alpha_q\beta_q = q\langle q\rangle$. Since $q \equiv 1 \bmod p$ and α_q, β_q are distinct, this is a contradiction. This ensures that we only need to consider the forms coming from $\Gamma_H(N)$, and get the isomorphism.

Let Δ_q, δ_q, and $\Delta_Q := \prod_{q\in Q}\Delta_q$ be as in §1, and

$\chi_q : G_{\Sigma\cup Q} \to \mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q}) \simeq (\mathbf{Z}/q\mathbf{Z})^\times \xrightarrow{\text{proj.}} \Delta_q$,

$\chi_Q := \prod_{q\in Q}\chi_q : G_{\Sigma\cup Q} \to \mathcal{O}[\Delta_Q]^\times$.

By abuse of notation we also use

$\chi_Q : G_{\Sigma\cup Q} \to T_Q^\times$.

for its composition with

$i : \mathcal{O}[\Delta_Q] \to T_Q$; $[a] \mapsto \langle x_a\rangle$,

where x_a is an integer such that $x_a \equiv a \bmod Q$ and $x_a \equiv 1 \bmod N$.

Let $H^1(X_{H'}(Nq), \mathcal{O})_m$ be the m-adic completion of $T_{H'}(Nq)$-module $H^1(X_{H'}(Nq), \mathcal{O})$, and let M_Q be the minus part $H^1(X_{H'}(Nq), \mathcal{O})_m^-$ with respect to the complex conjugation. Since $T_{H'}(Nq) \otimes_{\mathbf{Z}} \mathcal{O}$ decomposes into a product of local rings containing T_Q as a component, for the corresponding idempotent e $M_Q = eH^1(X_{H'}(Nq), \mathcal{O})^-$. $\mathrm{Hom}_{\mathbf{Z}}(T_{H'}(Nq), K) = S_{2,K}$ is the space of K-valued weight 2 cusp forms.

By the Shimura isomorphism

$$H^1(X_{H'}(Nq), \mathbf{C}) = S_{2,\mathbf{C}} \oplus \overline{S_{2,\mathbf{C}}}$$

$H^1(X_{H'}(Nq), \mathbf{R})^- \simeq H^1(X_{H'}(Nq), \mathbf{R})^+ \simeq S_{2,\mathbf{R}}$ as $T_H(Nq)$-modules, and we get that $T_{H'}(Nq) \otimes_{\mathbf{Z}} \mathbf{Q}$ is Gorenstein, and $S_{2,\mathbf{Q}}$ is free of rank one as a $T_{H'}(Nq) \otimes_{\mathbf{Z}} \mathbf{Q}$-module. Tensoring K and applying the projector e this implies that $M_Q \otimes_{\mathcal{O}} K$ is a free rank 1 $T_Q \otimes_{\mathcal{O}} K$-module. Then

Proposition.

M_Q is a free $\mathcal{O}[\Delta_Q]$-module.

Set $Y_Q = Y_{H'}(Nq)$, $Y_{Q-} = Y_H(N, q)$.

To show the proposition, it suffices to see

Lemma.

$H^1(Y_Q, \mathcal{O})^-$ is a free $\mathcal{O}[\Delta_Q]$-module with rank equal to the $\mathcal{O}$-rank of $H^1(Y_{Q-}, \mathcal{O})^-$.

proof)

Δ_Q-covering $\pi : Y_Q \to Y_{Q-}$ is defined over $\mathbf{R}$. (Assume Δ_Q-action is free.)

Then there exists a perfect $\mathcal{O}[\Delta_Q]$-complex L with $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$-action such that

$H^i(L) = H^i(Y_Q, \mathcal{O})$. $L^-=$ the minus part.

$H^i(L^- \otimes^{\mathbf{L}} \mathcal{O}[\Delta_Q]/m) = H^i(Y_Q, k)^- = 0$ except $i = 1$

This implies that $H^1(L^-) = H^i(Y_Q, \mathcal{O})^-$ is a free $\mathcal{O}[\Delta_Q]$-module.

We need to check TW2: $T_Q/(\delta_q - 1,\ q \in Q) = T$.

This is not evident since $T_Q/(\delta_q - 1,\ q \in Q)$ can have p-torsion a priori.

Assume $p \nmid N$. Then $\mathrm{Hom}_{\mathbf{Z}}(T_{H'}(Nq), \mathbf{Z}_p)$ is identified with $H^0(\mathcal{X}_{H'}(Nq)_{\mathbf{Z}_p}, \Omega^1)$ using the q-expansion principle. Here $\mathcal{X}_{H'}(Nq)_{\mathbf{Z}_p}$ is the $\mathbf{Z}_p$-model of $X_{H'}$. The action of Δ_Q is etale on $\mathcal{Y}_{H'}(Nq)_{\mathbf{Z}_p}$ (assume the action is free), and extends to $\mathcal{X}_{H'}(Nq)_{\mathbf{Z}_p}$. $\mathcal{X}_{H'}(Nq)_{\mathbf{F}_p}/\Delta_Q = \mathcal{X}_H(N, q)_{\mathbf{F}_p}$. Using base change, $\otimes\mathbf{F}_p$ of the map

$$\mathrm{Hom}_{\mathbf{Z}}(T_H(N), \mathbf{Z}_p) = H^0(\mathcal{X}_H(N, q)_{\mathbf{Z}_p}, \Omega^1)$$

$$\to \mathrm{Hom}_{\mathbf{Z}}(T_{H'}(Nq), \mathbf{Z}_p) = H^0(\mathcal{X}_{H'}(Nq)_{\mathbf{Z}_p}, \Omega^1)$$

equals to

$$H^0(\mathcal{X}_H(N,q)_{\mathbf{F}_p}, \Omega^1) \to H^0(\mathcal{X}_{H'}(Nq)_{\mathbf{F}_p}, \Omega^1).$$

The Δ_Q-invariants of $H^0(\mathcal{X}_{H'}(Nq)_{\mathbf{F}_p}, \Omega^1)$ coincides with $H^0(\mathcal{X}_H(N,q)_{\mathbf{F}_p}, \Omega^1)$ using $H^0(\mathcal{Y}_{H'}(Nq)_{\mathbf{F}_p}, \Omega^1)^{\Delta_Q} = H^0(\mathcal{Y}_H(N,q)_{\mathbf{F}_p}, \Omega^1)$ and looking at the regularity at cusps.

$$\mathrm{Hom}(T_{H'}(Nq), \mathbf{F}_p)^{\Delta_Q} = \mathrm{Hom}(T_{H'}(Nq)/(\delta_q - 1, q \in Q), \mathbf{F}_p)$$

Then $T_{H'}(Nq)/(\delta_q - 1, q \in Q) \otimes \mathbf{F}_p = T_H(N,q) \otimes \mathbf{F}_p$, and the claim follows.

If $p|N$, we need a refined argument, since the q-expansion principle is non-trivial in this case.

§5. Finding $\mathcal{Q}$

The essential point is that we have a deformation $\rho_Q^{mod} : G_{\Sigma \cup Q} \to \mathrm{GL}_2(T_Q)$ of $\bar{\rho}$ over T_Q by the method of pseudo-representations, whose local behavior can be understood by the local Langlands correspondence. Using Galois cohomology groups (and Chebotarev density theorem) we can choose an infinite set of appropriate Q's, assuming that the Hecke ring is minimal. We need the minimality here since the residual representation does not tell the size of the local deformation at each prime where the representation is unramified. There is another reason for ramified places.

Looking at the representation $\rho_Q^{mod} : G_{\Sigma \cup Q} \to \mathrm{GL}_2(T_Q)$ only is not quite enough (we do not want to deform the determinant), and we need to look at $\rho'_Q := \rho_Q^{mod} \otimes \chi_Q^{-1/2}$.

Theorem (Taylor-Wiles).

Assume $\bar{\rho}|_{\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p}\,)}$ is absolutely irreducible, $\bar{\rho}$ is flat or ordinary at p, and is of type (A), (B) or (C) at every $q \neq p$, $q|N$. T is a complete intersection if the representation is minimal.

proof) One already has a Taylor-Wiles system for T. Under the minimality we find a subset $Q \subset \mathcal{Q}_{\Sigma,\bar{\rho}}$ satisfying the assumption of the complete intersection theorem. Let $\rho'_Q : G_{\Sigma,Q} \to \mathrm{GL}_2(T_Q)$ be the twisted representation. The twist must be of type $\mathcal{D}$ (the minimal one) outside Q, and at primes $q \in Q$, its restriction to D_q must have the form $\begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$, where $\chi_1\chi_2$ is unramified at q. The local deformation data $\mathcal{D}_Q$ is defined as follows:

For $q \in \Sigma$, the condition is the same, and for $q \in Q$ we put no restriction on the deformation.

We denote by $\mathcal{D}^*$ and $\mathcal{D}^{*Q}$ the dual data of $\mathcal{D}$, $\mathcal{D}_Q$ as in [W], and for the dual $ad^0\bar{\rho}^* = ad^0\bar{\rho}(1)$ of $ad^0\bar{\rho}$, $H^1_{\mathcal{D}^*}(\mathbf{Q}_\Sigma/\mathbf{Q}, ad^0\bar{\rho}^*)$, $H^1_{\mathcal{D}^{*Q}}(\mathbf{Q}_{\Sigma\cup Q}/\mathbf{Q}, ad^0\bar{\rho}^*)$ are the dual Selmer groups.

Recall that

$$(m_{R_Q}/(m_{R_Q}^2, \lambda))^* = H^1_{\mathcal{D}_Q}(\mathbf{Q}_{\Sigma\cup Q}/\mathbf{Q}, ad^0\bar{\rho}),$$

where $R_{\mathcal{D}_Q}$ is the universal local deformation space of $\bar{\rho}$ of type $\mathcal{D}$. Let $\rho_Q^{univ} : G_{\Sigma\cup Q} \to \mathrm{GL}_2(R_{\mathcal{D}_Q})$ be the universal representation.

Put

$$r = \dim_k H^1_{\mathcal{D}}(\mathbf{Q}_\Sigma/\mathbf{Q}, ad^0\bar{\rho}).$$

Since ρ'_Q is a deformation of $\bar{\rho}$ of type $\mathcal{D}_Q$, we have a canonical map $R_{\mathcal{D}_Q} \to T_Q$. Note that the map is surjective, since $T_Q = T'_Q$ is generated by $\{T_\ell, \ell \notin \Sigma \cup Q\}$, which is the image of $\{\mathrm{trace}\,\rho_Q^{univ}(\mathrm{Fr}_\ell), \ell \notin \Sigma \cup Q\}$. Since $R_{\mathcal{D}_Q}$ is generated by at most $\dim_k H^1_{\mathcal{D}_Q}$ elements, T_Q is the same. The theorem is proved if we choose $Q \subset \{q : q \equiv 1 \bmod p^m\} \cap \mathcal{Q}_{\Sigma,\bar{\rho}}$ such that $\#Q = \dim_k H^1_{\mathcal{D}_Q}(\mathbf{Q}_{\Sigma \cup Q}/\mathbf{Q}, ad^0\bar{\rho}) = r$ for any $m \geq 1$.

By the minimality of $\mathcal{D}$, we have $\dim_k H^1_{\mathcal{D}}(\mathbf{Q}, ad^0\bar{\rho})/H^1_{\mathcal{D}^*}(\mathbf{Q}, ad^0\bar{\rho}^*) = 0$. For $\mathcal{D}_Q$, we have, by the formula of [W]

$$\dim_k H^1_{\mathcal{D}_Q}/H^1_{\mathcal{D}^*Q} = \dim_k H^1_{\mathcal{D}}(\mathbf{Q}, ad^0\bar{\rho})/H^1_{\mathcal{D}^*}(\mathbf{Q}, ad^0\bar{\rho}^*) + \sum_{q \in Q} \dim_k H^0(\mathbf{Q}_q, ad^0\bar{\rho}^*)$$

$$= \sharp Q.$$

Note that $\dim_k H^0(\mathbf{Q}_q,\ ad^0\bar{\rho}^*) = 1$ for each $q \in Q \in \mathcal{Q}_{\Sigma,\bar{\rho}}$, since $ad^0\bar{\rho}^*(\mathrm{Fr}_q)$ has eigenvalues $q\alpha_q/\beta_q, q, q\beta_q/\alpha_q$.

So, to have $\#Q = \dim_k H^1_{\mathcal{D}_Q} = r$, it is enough to have $H^1_{\mathcal{D}^*Q} = 0$ and $\#Q = r$. We apply the following proposition.

Proposition.
Assume $\bar{\rho}|_{\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p}\,))}$ is absolutely irreducible. Then there is $Q \subset \{q : q \notin \Sigma, q \equiv 1 \bmod p^m\} \cap \mathcal{Q}_{\Sigma,\bar{\rho}}$ such that

$$H^1_{\mathcal{D}^*}(\mathbf{Q}_\Sigma/\mathbf{Q}, ad^0\bar{\rho}^*) \to \prod_{q \in Q} H^1_f(\mathbf{Q}_q,\ ad^0\bar{\rho}^*)$$

is injective (and hence the kernel $H^1_{\mathcal{D}^*Q}$ vanishes).

This proposition is proved by a closer study of subgroups of GL_2 of a finite field and Chebotarev density theorem. The assumption on $\bar{\rho}|_{\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p}\,))}$ is necessary only when the projective representation associated to $\bar{\rho}$ has $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ as the image.

Since $\dim_k H^1_f(\mathbf{Q}_q,\ ad^0\bar{\rho}^*) = \dim_k H^0(\mathbf{Q}_q,\ ad^0\bar{\rho}^*) = 1$ for each $q \in Q$, we can shrink Q so that

$$H^1_{\mathcal{D}^*}(\mathbf{Q}_\Sigma/\mathbf{Q}, ad^0\bar{\rho}^*) \ \simeq\ \prod_{q \in Q} H^1_f(\mathbf{Q}_q, ad^0\bar{\rho}^*).$$

Then we have $\#Q = \dim_k H^1_{\mathcal{D}^*}(\mathbf{Q}_\Sigma/\mathbf{Q}, ad^0\bar{\rho}^*) = r$ using $\dim_k H^1_f(\mathbf{Q}_q,\ ad^0\bar{\rho}^*) = 1$ again.

This completes the proof of the Theorem.

§6. Mazur conjecture : $R_{\mathcal{D}} \simeq T$

Finally we prove the Mazur conjecture in the case of the minimal Hecke algebras. The argument here is due to Faltings. Recall that deformation ring $R_{Q_{m(n)}}$ is generated by at most r elements.

Suppose now that we have a similar diagram for deformation rings

$$\begin{array}{ccccccc} (R_{Q_{m(n)}}/I_n)^r & \xrightarrow{f} & R_{Q_{m(n)}}/I_n & \longrightarrow & R/I_n & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ (T_{Q_{m(n)}}/I_n)^r & \longrightarrow & T_{Q_{m(n)}}/I_n & \longrightarrow & T/I_n & \longrightarrow & 0 \end{array}$$

such that f looks like $(\delta_1 - 1, .., \delta_r - 1)$. Then R will be a complete intersection of the same defining equations as T (we argue similarly as in §1), hence $R \simeq T$ follows. We need to define elements $\delta_1, \cdots, \delta_r \in R_{Q_{m(n)}}$ such that $R_{Q_{m(n)}}/(\delta_1 - 1, .., \delta_r - 1) \simeq R$.

Recall first what $\delta_q \in T$ is : The representation $\rho_Q : G_{\Sigma \cup Q} \to \mathrm{GL}_2(T_Q)$, restricted to the inertia group I_q at q, factors through $\mathrm{Gal}(\mathbf{Q}_q^{unr}(\zeta_q)/\mathbf{Q}_q^{unr})$. Let σ_q be a generator of a Sylow p-subgroup of this Galois group. Then $\delta_q \in T$ is such that

$$\rho_Q(\sigma_q) = \begin{pmatrix} \delta_q & 0 \\ 0 & 1 \end{pmatrix}.$$

Now let $\rho_Q^{univ} : G_{\Sigma \cup Q} \to \mathrm{GL}_2(R_{\mathcal{D}_Q})$ be the universal representation of type $\mathcal{D}_Q$ with residual representation ρ. By assumption, $\rho(\mathrm{Fr}_q)$ has distinct eigenvalues α_q and β_q. We take a basis so that $\rho_Q^{univ}(f) = \begin{pmatrix} a_q & 0 \\ 0 & b_q \end{pmatrix}$, where f is a Frobenius lift in D_q.

Claim.
$\rho_Q^{univ}|_{D_q}$ is diagonal.

Proof. $\rho_Q^{univ}|_{I_q}$ factors through a pro-p group, so it factors through $\mathbf{Z}_p(1)$ (= the Galois group of the $\mathbf{Z}_p$-extension of $\mathbf{Q}_q^{unr}$). Let σ be a generator of this group. We have $f\sigma f^{-1} = \sigma^q$. We will check modulo m^n, inductively on n, that $\rho_Q^{univ}(\sigma)$ is diagonal.

$\rho_Q^{univ}(f\sigma f^{-1}) = \rho_Q^{univ}(\sigma^q)$. Writing down this relation explicitly, we have the claim.

The twist $\rho'_Q = \rho_Q \otimes \chi_Q^{-1/2}$ looks as

$$\rho'_Q(\sigma_q) = \begin{pmatrix} \delta_q^{1/2} & 0 \\ 0 & \delta_q^{-1/2} \end{pmatrix}.$$

So, if

$$\rho_Q^{univ}|_{D_q} \simeq \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix},$$

we set $\delta_q := \psi_1(\sigma_q)^2 \in R_{\mathcal{D}_Q}$. Then we have $R_{\mathcal{D}_Q}/(\delta_1 - 1, .., \delta_r - 1) \simeq R_{\mathcal{D}}$.

References

[Car] H. Carayol, Sur les représentations p-adiques associées aux formes modulaires de Hilbert, Ann. Sci. Ec. Norm. Sup. IV, Ser 19 (1986), 409-468.
[D] F. Diamond, On deformation rings and Hecke rings, November 1994
[Ma] H. Matsumura, Commutative algebra,
[TW] R. Taylor, A. Wiles, Ring theoretic properties of certain Hecke algebras, Ann. of Math.,(1995)
[W], A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math., (1995)